

Міністерство освіти і науки України Національний технічний університет України  
"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

## «Криптографія»

Лабораторна робота №3

«Криптоаналіз афінної біграмної підстановки»

Виконав

студент групи ФБ-93

Флекевчук Данило

Київ – 2021

**Мета:** набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанування прийомами роботи в модулярній арифметиці.

**Завдання:**

- уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- реалізувати підпрограми із необхідними математичними операціями: обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
- за допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифротексту (2 варіант).
- перебрати можливі варіанти співставлення частих біграм мови і частих біграм шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співпадиння знайти можливі кандидати на ключ (a, b) шляхом розв'язання системи.
- для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російської мовою, відкинути цього кандидата.
- повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

**Хід роботи:**

**Частина 1.**

В файлі main.py я створив всі функції для того, щоб порахувати НСД, зворотній елемент за розширеним алгоритмом Евкліда, розв'язати лінійне рівняння за модулем M.

**Частина 2.**

Перш ніж перейти до підбору ключів потрібно знайти 5 найчастіших біграм ШТ. Їм у відповідність поставлять біграми ВТ, які скоріш за все є 5 найпопулярнішими в мові ВТ.

ШТ	ВТ
тд	ст
рб	но
во	ен
щю	ни
ет	от

Найчастіші біграми ШТ було отримано програмно. Для ВТ було взято список біграм з літератури.

**Частина 3.**

Тепер підбір та перевірка ключів. Знайдемо всі ключі через перестановки біграм. Для отримання ключа ми будемо переставляти біграми з ШТ. Та розв'язувати серію з 4 систем.

тд	рб	во	щю	ет
ст	но	ен	ни	от

→

тд	рб	во	ет	щю
ст	но	ен	ни	от

З таких маніпуляцій я отримав список ключів.

Всі ймовірні ключі

42, 805	52, 262	64, 717	106, 948	120, 494	172, 913	183, 570	184, 649	199, 700
223, 819	236, 107	251, 886	265, 820	289, 60	371, 576	406, 827	407, 892	435, 731
448, 828	449, 563	512, 317	513, 803	526, 900	554, 318	555, 474	590, 159	672, 578
696, 876	710, 91	725, 466	738, 547	762, 510	777, 652	778, 489	789, 686	841, 872
855, 586	897, 342	909, 618	919, 172					

Тепер потрібно їх перевірити. Для цього я проводжу аналіз отриманого тексту на найчастіші біграми (Analis). Якщо в тексті найчастішими біграмами є ті, які є в списку 10 найчастіших біграм мови => наш текст є російською мовою. Хоча шанс отримання нісенітниць за такої перевірки залишається, він значно менший за її відсутності.

#### Частина 4.

Після попередніх кроків у мене був кандидат лише один. Він мав співпадіння на 4 біграми з 5 при розшифруванні ним. Він виник на перестановці ['ст', 'но', 'ен', 'ни', 'от']. Ключ мав вигляд A=199 B=700.

ВТ:

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекавовсякомслучаеонегоглавныйисточникчувствавиныиизвестноеединственныйлиисследованиемнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупленияиотнодьянесущественноеединственныйлиэтоисточникпсихологическоеположениесложноиуждаетсявобъясненияхотношениемальчикакотцакакмыговоримамбивалентнопомимоненавистииззакоторойхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекотораядолянежностикнемуоботношениясливаютсяидентификациюотцомхотелосьбызанятьместоотцапотомучтоонвызываетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянакрупноепрепятствиевопределенныймоментребенокначинаетпониматьчтопопыткаустранитьотцакаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизстрахакастрацияэтоествинтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерьюиотустраненияотцапосколькуэтожеланиеостаєтьсяобластибессознательногооноявляетсяосновойдляобразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудьбукакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдальнейшиеосложненияеслиуробенкасильнееразвитконституционныйфакторназываемыйнамибисексуальностьюотогдаподугрозойпотери мужественностичерезкастрациюукрепляетсятенденцияуклонитьсявсторонуженственностиболее тоготенденцияпоставитьсебянаместоматерииперенятьееролькакобъекталюбвиотцаоднализьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпонимаетчто...

#### Висновки:

В цій роботі я закріпив знання з статистичного аналізу тексту. Ознайомився з методом атаки на шифр афінної біграмної підстановки. Також я повторив знання з модульної арифметики. Бонусом дізнався про можливості стандартних бібліотек пайтону.